

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:) Group Art Unit: 2135
John LEONARD *et al.*) Examiner: B. Dada
Serial Number: 09/390,363) Attorney Docket: LEON3001beu
Filed: September 7, 1999) Confirmation No.: 6725

For: System And Method For Enabling The Originator Of An Electronic Mail Message To Preset An Expiration Time, Date, And/Or Event, And To Control Processing Or Handling By A Recipient

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Honorable Commissioner For Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

Applicant requests review of the final rejection in the above-identified application.
No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reasons stated on the attached sheets (no more than 5 pages are provided).

I am the attorney or agent of record.

Respectfully submitted,

BACON & THOMAS, PLLC

Date: August 23, 2005

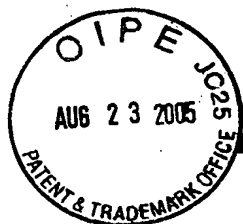
By: BENJAMIN E. URCIA
Registration No. 33,805

Serial Number 09/390,363

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending L...PULLEONARD390363\preab.wpd



REASONS FOR REQUESTING REVIEW OF THE FINAL REJECTION

(Attachment to Pre-Appeal Brief Request for Review)

Review of the final rejection of claims 1-50 under 35 USC §103(a) in view of U.S. Patent Nos. 6,442,600 (Anderson) and 6,487,586 (Ogilvie) is requested on the grounds that neither the Anderson patent nor the Ogilvie patent discloses or suggests use of a viewer applet installed on a recipient's computer that enables the originator of an e-mail message to control viewing of the message before the occurrence a date, time, or event by enabling decryption of the message before the date, time, or event, and by preventing decryption of the message after the date, time, or event.¹ Instead, the Anderson patent teaches encryption and decryption of messages by a web browser, together with message deletion after an expiration date, *but fails to associate the encryption/decryption feature of the browser with the message expiration feature* (which is the basis principle of the present invention). The Ogilvie clearly does not suggest modification of the message deletion feature of Anderson, by suggesting use of Anderson's decryption software as a viewer applet to implement processing controls set by the message originator, since the Ogilvie patent merely discloses a method and system in which e-mail that is not read is automatically deleted. In other words:

- the claimed invention uses a viewer applet on the recipients computer to control viewing by only decrypting a message before a date, time or event selected by the message originator,

whereas:

¹ Claim 1, for example, includes the following clause, positively reciting this feature of the invention: "...wherein said viewer applet is arranged to **decrypt** said electronic mail message to permit viewing of said electronic mail message before the occurrence of the **date, time, or event selected by said originator of the electronic mail message**, and to **prevent decryption** and viewing of said encrypted electronic mail message by said recipient after the occurrence of the date, time, or event selected by said originator of the electronic mail message, . . ."

- Anderson teaches message deletion after an expiration date, but fails to ensure deletion by using a viewer applet and decryption control, as claimed (Anderson's deletion can easily be over-ridden by the recipient), and
- Ogilvie does not make up for this deficiency of Anderson since Ogilvie fails to teach message deletion after an expiration date, or use of decryption to ensure such deletion. Ogilvie teaches message deletion that is entirely under the control of the recipient—if the recipient reads the message, then it is not deleted—which is exactly contrary to the claimed invention's use of decryption to enable *sender* rather than *recipient* control of the message, and therefore Ogilvie could not possibly have suggested modification of Anderson's message deletion to ensure deletion by preventing decryption of the message after the expiration date.

The deficiencies of the applied references may be summarized as follows:

- a. Anderson teaches encryption and decryption of e-mail, and deletion of messages after an expiration date, but does not think to use decryption (*i.e.* prevention of decryption) to ensure that the message cannot survive the expiration date; and
- b. Ogilvie places no limitations are placed on viewing of the message by the recipient, and therefore could not have suggested modification of the system of Anderson to use encryption/decryption to implement such limitations.

Indeed, inclusion of viewing controls would be **contrary** to the purpose of the Ogilvie system, **which is to avoid annoying persons who do not wish to read an e-mail by eliminating the need to positively delete the e-mail if deletion is desired.** The sender presumably wants recipients to read the e-mail and places absolutely no restrictions on doing so, but merely makes it convenient to automatically delete the e-mail if viewing is not desired. **In contrast, the claimed invention forces deletion even if viewing is desired, which is exactly contrary to Ogilvie.**

The Examiner is correct that the Anderson patent discloses a web browser, expiration periods, and decryption. However, the invention is not, as suggested by the Examiner, a web browser, electronic message expiration, and decryption. The fact the Anderson teaches these elements is irrelevant to the invention. The applicant has not suggested that it invented either a web browser, message encryption, or message expiration. What the applicant has invented is a way to **ensure** electronic message expiration by causing the applet that decrypts the message to stop decrypting the message after an expiration date established by a sender of the message.

It might be possible, with respect to the broader claims, to interpret an “applet” as a browser. However, **no browser is equipped to prevent decryption of a message based on a date entered by a sender of the message, as claimed.** Furthermore, a number of claims recite the feature in which the applet is downloaded from a central mail server and cooperates with the mail server to implement the expiration by decrypting the message based on key exchange *with the server* (no conventional browser is downloaded from a mail server and implements an expiration date in cooperation with the server in the manner claimed).

Even though the Anderson patent mentions encryption and decryption, the encryption and decryption is not associated with message expiration. Instead, Anderson teaches, essentially, **voluntary** message deletion at the expiration date. It does not teach or suggest the basic principle of the invention, which is to effectively cause a message to expire by preventing decryption of the message after the expiration date. As pointed out in the previous response, the Anderson patent merely gives the recipient the option of having a message automatically deleted on the expiration date or of saving the message. The recipient is not prevented from doing anything that he or she wants to do with the message, and encryption is not involved in expiration of the message or in preventing the recipient from circumventing expiration controls by simply copying or saving the message and viewing it after the expiration date.

The purpose of the system of Anderson is to save **recipients** the trouble of storing, managing, and protecting received messages, as explained in col. 1, lines 20-29 and in particular in col. 1, lines 65 *et seq.* of the Anderson patent.

. . .The recipient can also provide various instructions about actions to be taken with the message corresponding to an indicator, such as to save or delete the message or to forward the message to another recipient. In one embodiment, after all recipients have reviewed the message and no recipient has currently indicated to save the message (or all have indicated to delete the message), the system then deletes the single copy of the message).

Nowhere does this passage (or any other passage in Anderson) disclose or suggest that tracking and management of messages is in response to controls selected by the originator or sender of the message **and implemented by means of encryption and a viewer applet on the recipient's computer.**

To implement the system of Anderson, there is **no need** for decryption to prevent viewing of a message except via a "viewer applet" that limits message access by the recipient. The only encryption provided for is encryption at the request of the recipient to limit viewing by third parties rather than the recipient. There are no limits on viewing of the message by the recipient, and any limitations that are selected by the message originator or sender are implemented by a message tracking table rather than a viewer applet, as claimed, that decrypts the message at the recipient's computer. Since the only use of an expiration date in the system taught by the Ogilvie patent is so that the recipient does not have to bother with manual deletion of the e-mail, Ogilvie could not possibly have suggested modifying the system of Anderson to obtain the claimed invention. **As disclosed by Ogilvie, the recipient is free to over-ride the expiration date and continue viewing the e-mail.** In contrast, the claimed invention seeks to provide absolute originator-control of the expiration date, so that it is impossible for the recipient to prevent expiration. This is accomplished by encrypting the message so that it can only be read by a viewer applet arranged to implement the

Serial Number 09/390,363

*Attachment to Pre-Appeal Brief
Request for Review*
Examiner B. Dada
Group Art Unit 2135

originator-controls. Neither prior art reference suggests such an applet, and therefore reconsideration and withdrawal of the final rejection is requested.